Location Based Encryption & Its Role In Digital Cinema Distribution

Logan Scott, *GeoCodex LLC, LS Consulting*
loganscott53@earthlink.net
Dorothy E. Denning, *GeoCodex LLC, Naval Postgraduate School*
ded@denningassociates.com

BIOGRAPHY

Logan Scott is a consultant specializing in radio frequency signal processing and waveform design for communications, navigation, radar, and emitter location. He has more than 25 years of military GPS systems engineering experience. As a senior member of the technical staff at Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers using large-scale application-specific integrated circuit (ASIC) technologies. He has developed gain and frequency plans, non-uniform analog/digital conversion techniques, fast acquisition architectures, Baseband signal processing algorithms and adaptive array approaches. He is currently involved in projects to provide location based encryption and authentication. He holds 28 US patents.

Dr. Dorothy E. Denning is a founding partner in GeoCodex and a professor in the Department of Defense Analysis at the Naval Postgraduate School. Her current work encompasses the areas of cybercrime and cyberterrorism, information warfare and security, and cryptography. She has published 120 articles and four books, her most recent being Information Warfare and Security. She is an ACM Fellow and recipient of several awards, including the Augusta Ada Lovelace Award and the National Computer Systems Security Award. In November 2001, she was named a Time magazine innovator. Dr. Denning received the B.A. and M.A. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University. She has previously worked at Georgetown University, Digital Equipment Corporation, SRI International, and Purdue University. She holds 1 US patent.

ABSTRACT

Each year, film studios spend over $1 billion on the mechanics of duplicating and distributing films to exhibition venues located across the U.S. With the advent of digital cinema projectors, much of this expense can be eliminated through more cost efficient digital distribution methods.

SATCOM links provide for a very efficient and cost effective digital cinema distribution model but piracy is a major concern; SATCOM links are easy to intercept and loss of a pristine, successful, first run film to pirates could have major financial repercussions. The experience with Direct Satellite Services (DSS) has not been encouraging. There are an estimated 3 million unauthorized users using cloned versions of the tamper resistant smart cards that seek to prevent this. Furthermore, cinema stakeholders are risk adverse towards piracy based on the music industry's experience with Napsterization. Music sales are down for the fourth year in a row (9% in 2002) and company valuations are down 40%, in part because of piracy.

As a consequence, there has been significant interest in providing location-based security for digital cinema distribution and forensic analysis in the event of piracy. In this application, the same, large (25 to 190 Gbyte), encrypted media file might be used at multiple theatre locations nationwide but with distinct GeoLocked keys specific to the intended recipient location and its exhibition license. This provides a secure and efficient point-to-multipoint distribution model for delivery via satellite or DVD. At the exhibition hall, robust watermarking/steganographic techniques can introduce location, time and exhibition license information into the exhibition for subsequent use in piracy investigations.

This paper starts by describing a geo-encryption approach that builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Location Based Encryption & Its Role In Digital Cinema Distribution	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
ION GPS/GNSS 2003, September 9-12, Portland, OR

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**1**	**10**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

location(s) or for specific area(s), e.g. a studio's campus area. Constraints in time and velocity as well as location can also be enforced. We then discuss a process of applying successive geo-encryptions at the originating node to enforce specific geographic routings for transmission to the final destination node.

We then describe the process of creating and distributing digital cinema content with an eye towards security requirements. One of the more difficult issues is the large number of mutually mistrustful parties involved in the process. We specifically show how time & location constraints introduced via geo-encryption can provide architectural features needed to allow untrusted parties to act cooperatively to bring the exhibition to the screen while maintaining a high degree of protection against piracy. Suborning a single party does not lead to "loss of the film". We also show how these mechanisms can help protect the fiduciary interests of the various parties by giving each an enforceable say in whether or not the exhibition can proceed.

INTRODUCTION

Pirated versions of "Star Wars: Attack of the Clones" were available on the Internet two days before its first theatrical release. At advance screenings of "Finding Nemo", Disney hired security firm Burns Pinkerton to screen audiences using metal detectors and night vision goggles. Specifically, they were looking for anyone carrying video recording equipment(s). The measures were effective; the first bootleg versions of "Finding Nemo" didn't show up on the Internet until two days after the first theatrical release.

Piracy is a real and growing concern to the film industry. According to Rich Taylor, a spokesman for the MPAA, "It's estimated we lose between $3 billion and $4 billion a year to this problem despite strong anti-piracy actions by the movie industry." [Reuters, May 30, 2003]

The advent of digital cinema projection systems could exacerbate the problem; loss of a pristine, successful, first run film to pirates could have major financial repercussions. Bootleg versions generally have poor video and sound quality and do not demand high street prices. Pirates who successfully capture the original digital version of a theatrical release could create DVD quality versions demanding a higher street price. Additionally, many buyers of bootleg versions later purchase the commercial DVD release because of quality issues. Improved bootleg quality would lessen their incentive to purchase authorized DVD versions.

Compounding the issue, cost effective digital cinema distribution methods favors transmission methods subject to easy interception. Satellite transponder signals are readily intercepted using receiver technology comparable to that used in DSS. DVDs can be duplicated on a $300 DVD Recorder.

In spite of all these issues (or because of them), there is strong motivation to widely deploy digital cinema. Each year, film studios spend over $1 billion on the mechanics of duplicating and distributing films to exhibition venues located across the U.S. With the advent of digital cinema projectors, much of this expense can be eliminated through more cost efficient digital distribution methods.

At the same time, digital cinema can provide an avenue for incorporating additional security features not available with the current "analog" distribution chain. Highly secure encryption and authentication technologies can be used to thwart unauthorized access to digital films and persistent watermarking features can be used to discourage bootlegging and assist prosecution efforts. Precise location and timing information, when combined with extant security algorithms can promote these objectives by restricting access to certain locations and timeframes and is the primary topic of this paper.

GEOENCRYPTION

Geo-encryption builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing.

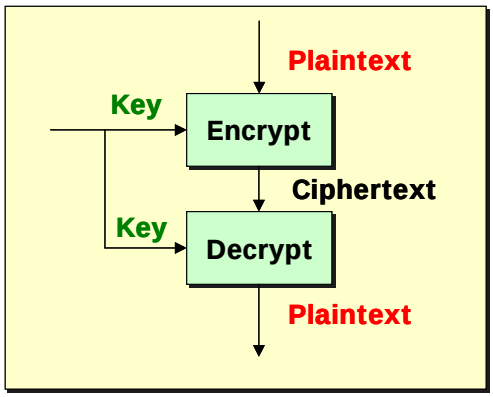
The term "location-based encryption" is used here to refer to any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system.

Location-based encryption can be used to ensure that data cannot be decrypted outside a particular facility, for example, at a particular theatre, the headquarters of a government agency or corporation, or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints may be placed on the decryption location.

A Short Tutorial On Encryption Algorithms

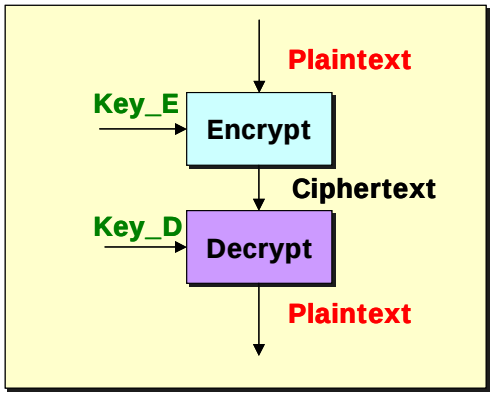
Encryption algorithms can be divided into two categories: symmetric algorithms and asymmetric algorithms. Referring to figure 1, symmetric algorithms use the same key for encrypting and decrypting plaintext. Numerous, very fast symmetric algorithms are in widespread use including: DES & Triple-DES as described in [1] and the newly released Advanced Encryption Standard (AES) described in [2]. Keeping the key private is essential to maintaining security and therein lies the crucial question: how to share keys securely. Numerous techniques have been developed and the interested reader is directed to [3] for further discussion.

Figure 1: Symmetric Algorithm



Asymmetric algorithms are comparatively new on the scene with the first published description [4] in 1976. Also known as Public Key algorithms, these algorithms have distinct keys for encryption and decryption as is shown in figure 2. Here, Key_E can be used to encipher the plaintext but not to decipher it. A separate key (Key_D) is needed to perform this function.

Figure 2: Asymmetric Algorithm

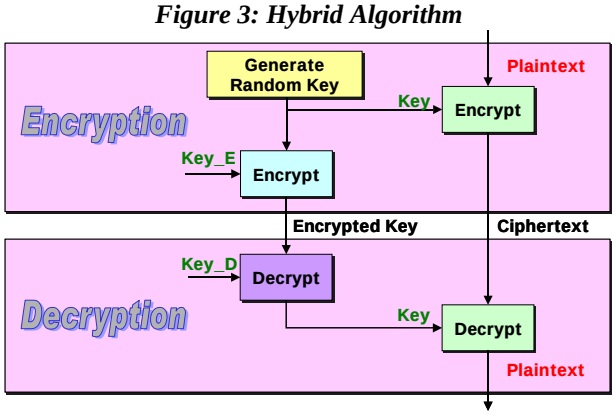


In principle, to securely convey the plaintext, the intended recipient could generate a key pair (Key_E, Key_D) and send Key_E, the public key, to the originator via unsecured channels. This would allow the originator (or anyone else) to encrypt plaintext for transmittal to the recipient who uses Key_D, the private key, to decrypt the plaintext.

RSA, named after its creators Rivest, Shamir & Adleman is perhaps the most popular asymmetric algorithm in use today. Its security is based on the difficulty of factoring large prime numbers.

One major drawback with asymmetric algorithms is that their computational speed is typically orders of magnitude (~1,000) slower than comparable symmetric algorithms. This has led to the notion of hybrid algorithms such as the one shown in figure 3.

Figure 3: Hybrid Algorithm



Here, a random key, sometimes called the session key, is generated by the originator and sent to the recipient using an asymmetric algorithm. This session key is then used by both parties to communicate securely using a much faster symmetric algorithm. The hybrid approach has found wide application, most notably on the Internet where it forms the basis for secure browsers (Secure Socket Layer (SSL)) and secure e-mail.

The GeoEncryption Algorithm

In principle, one could attach location and time specifications to the ciphertext file and build devices that would decrypt the file only when within the specified location & time constraints. There are several potential problems with such an approach:

- The resultant file reveals the physical location of the intended recipient. The military frowns on this sort of thing, at least for their own forces. Furthermore, it provides vital information to someone who wants to spoof the device.

- If the device is vulnerable to tampering, it may be possible to modify it so as to completely

bypass the location check. The modified device would decrypt all received data without acquiring its location and verifying that it is correct. Alternatively, an adversary might compromise the keys and build a modified decryption device without the location check. Either way, the modified device could be used anywhere and location would be irrelevant

As another possibility, one might consider using location itself as the cryptographic key to an otherwise strong encryption algorithm like AES. This is ill advised in that location is unlikely to have sufficient entropy (uncertainty) to provide strong protection. Even if an adversary does not know the precise location, there may be enough information to enable a rapid brute force attack analogous to a dictionary attack. For example, suppose that location is coded as a latitude-longitude pair at the precision of 1 centimeter, and that an adversary is able to narrow down the latitude and longitude to within a kilometer. Then there are only 100,000 possible values for each of latitude and longitude, or 10 billion possible pairs (keys). Testing each of these would be easy.

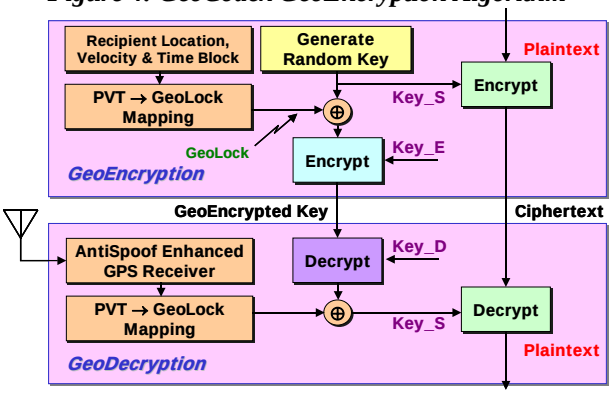
Applying an obfuscation function to the location value before using it as a key could strengthen this approach; however, the function would have to be kept secret in order to prevent the adversary from doing the same. In general, security by obscurity is scoffed at, because once the secret method is exposed, it becomes useless. The entire security system collapses like a house of cards.

A guiding principle behind the development of cryptographic systems has been that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public, only that they be designed to withstand attack under the assumption that the adversary knows them. Security is then achieved by encoding the secrets in the keys, designing the algorithm so that the best attack requires an exhaustive search of the key space, and using sufficiently long keys that exhaustive search is infeasible.

GeoCodex's GeoEncryption algorithm addresses these issues by building on established security algorithms and protocols. Referring to figure 4, our approach modifies the previously discussed Hybrid algorithm to include a GeoLock.

On the originating (encrypting) side, a GeoLock is computed based on the intended recipient's Position, Velocity, and Time (PVT) block. The PVT block defines where the recipient needs to be in terms of position, velocity & time for decryption to be successful. The GeoLock is then XORed with the session key (Key_S) to form a GeoLocked session key. The result is then encrypted using an asymmetric algorithm and conveyed

Figure 4: GeoCodex GeoEncryption Algorithm

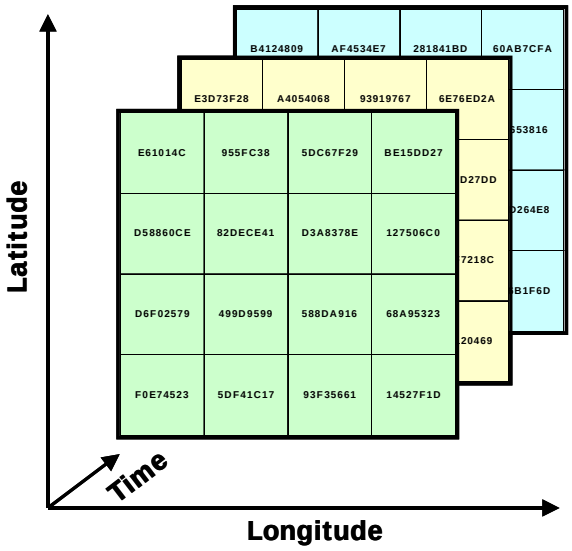


to the recipient, much like we saw in the Hybrid algorithm of figure 3. On the recipient (decryption) side, GeoLocks are computed using an AntiSpoof GPS receiver for PVT input into the PVT→GeoLock mapping function. If the PVT values are correct, then the resultant GeoLock will XOR with the GeoLocked key to provide the correct session key (Key_S).

PVT→GeoLock mapping function

Sidestepping the issue of what constitutes an AntiSpoof receiver for the moment, we now address how GeoLocks are formed. Figure 5 shows a notional diagram of a PVT→GeoLock mapping function where latitude, longitude and time constitute the inputs. Here, a regular grid of latitude, longitude and time values has been created, each with an associated GeoLock value.

Figure 5: PVT→GeoLock Mapping Function

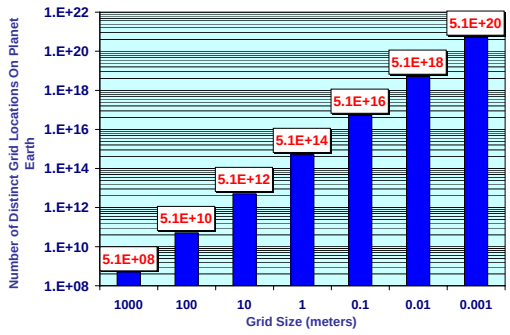


Grid spacing must take into account the accuracy of the GPS receiver at the decrypting site; otherwise erroneous GeoLock values may result. It makes no sense to have 1cm grid spacing if using a standalone GPS receiver.

Conversely, if using an RTK style receiver capable of 2cm accuracy, 10-meter grid spacing is overly conservative. Grid spacing may also be wider in the vertical direction to account for poorer vertical positioning accuracy typical in most sets because of satellite geometries [5].

Figure 6 shows the number of possible grid points on the planet as a function of grid spacing, ignoring altitude, time and velocity.

Figure 6: Number of Distinct Grid Locations



A more complete PVT→GeoLock mapping function could actually have eight inputs:

- Position (East, North, Up)
- Velocity (East, North, Up)
- Time
- Coordinate System Parameters

The velocity inputs might actually map into a minimum speed requirement so as to ensure that the recipient is actually underway. Including coordinate system parameters in the PVT→GeoLock mapping function provides support for non-stationary reference frames. This feature might be used, for example, in communicating through, or with, a satellite.

The grid could just as well be based on a Military Grid Reference System (MGRS) or it's close cousin UTM. In fact, any arbitrary shapes could have been used; for example the shape of the post production facility's campus could map to a single GeoLock value so as to permit successful decryption when located in the campus but not when outside.

Finally, we note that the PVT→GeoLock mapping function itself may incorporate a hash function or one-way function with cryptographic aspects in order to hinder using the GeoLock to obtain PVT block values. Similarly, the algorithm may be deliberately slow and difficult; perhaps based on solving a difficult problem.

A Few Quick Observations On AntiSpoof Receivers

Most civilian receivers are trivially simple to spoof; simply hook up one of the many excellent signal simulators available and the receiver will buy into whatever PVT values you want [6,7]. This is why military receivers use Y-code; an encrypted version of P-code. Unless the spoofer has access to the correct cryptographic keys and knows how to generate Y-code from P-code, it can't spoof the military set. He may be able to jam it, but not spoof it.

Current civil signal architectures provide no such protections; they operate without any security features whatsoever. The Galileo system is likely to incorporate some as yet undisclosed security features in their Commercial Services (CS) signals but thus far, attempts to incorporate security features into civil GPS have been rebuffed.

Civilian sets can be made difficult to spoof through a series of hardening measures. These include a variety of signal's checks:

- Use J/N meter to check for above normal energy levels
- Monitor C/No meter for Consistency/ Unexpected C/No given J/N
- Monitor Phase Difference Between Antenna Elements (All signals shouldn't come from the same direction)
- Deep Acquisition to Look for Weak, Real Signals

Numerous navigation checks can also be instituted:

- Compare "Watch Time" with "Signals Time" (Most signal generators can't synchronize with GPS time)
- Continuity Checks in Time and Position (There is no hyperspace button in real life)
- Consistency with other Navigation Sensors
- Large Residuals, Particularly in Differential Correction Channel(s)
- RAIM Type Functions

With careful attention to detail, civilian sets do not have to be as vulnerable to spoofing as most of them are.

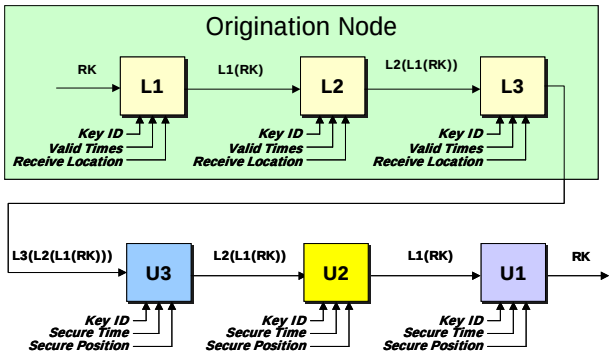
Relay Encryption to Force a Particular Routing & For Authentication

Successive Geo-encryption can be used to force data and/or keys to follow a specific geographical path before it can be decrypted. This is achieved by applying multiple geo-locks at the origination node prior to transmittal using a procedure such as the one shown in figure 7. As each

required node is traversed, one layer of GeoLocking is removed, thus ensuring the desired path has been followed.

Relay encryption might be useful for applications that employ regional distribution centers for the distribution of

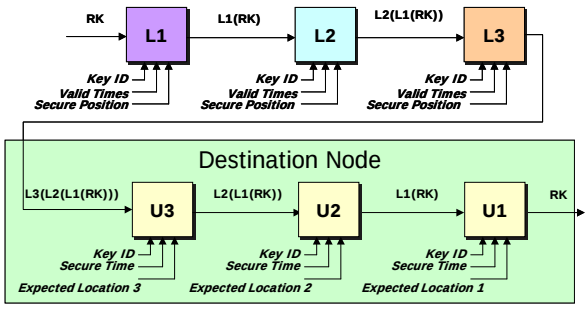
Figure 7: Successive GeoLocking to Force A Particular Routing



data supplied by producers. For example, in subscription television, the producers could be the television networks, while the distributors are cable or satellite television providers. A producer could lock a key initially to a geographic region covered by one of the distributors using a key known only to the subscribers, and then to the precise location of the distributor using the distributor's key. The distributor would unlock its geo-lock before broadcasting the programming to subscribers, who would then unlock the regional geo-lock and decrypt the ciphertext.

In some applications, it may be desirable to know that a message has followed a particular route. Figure 8 depicts a process similar to the Route Forcing technique for achieving this, where each traversed node in effect stamps the message with its PVT values.

Figure 8: Route Authentication By Successive GeoEncryption



DIGITAL CINEMA DISTRIBUTION

"Today, the film studios spend over $1 billion each year to duplicate, distribute, rejuvenate, redistribute and ultimately destroy the thousands of film reels required to bring the close to 500 films released each year to audiences across the U.S." Booz Allen Hamilton: DIGITAL CINEMA: BREAKING THE LOGJAM

SATCOM links provide for a very efficient and cost effective digital cinema distribution model but piracy is a major concern; SATCOM links are easy to intercept. The experience with Direct Satellite Services (DSS) has not been encouraging. There are an estimated 3 million unauthorized users using cloned versions of the tamper resistant smart cards that seek to prevent this. Furthermore, cinema stakeholders are risk adverse towards piracy based on the music industry's experience with Napsterization. Music sales are down 8% and company valuations are down 40%, in part because of piracy.

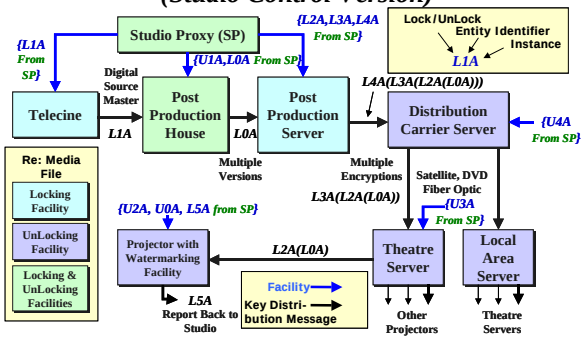
As a consequence, there has been significant interest in providing location-based security for digital cinema distribution and forensic analysis in cases of piracy. GeoCodex has been working with Digital Cinema Ventures (DCV) to develop security techniques specific to this industry.

In this application, the same, large (25 to 190 Gbyte), encrypted media file might be used at multiple theatre locations nationwide but with distinct GeoLocked keys specific to the intended recipient location and its exhibition license. This provides a secure and efficient point to multipoint distribution model applicable to distributions via satellite or DVD. At the exhibition hall, robust watermarking/steganographic techniques can introduce signed location, time and exhibition license information into the exhibition for subsequent use in piracy investigations.

Additionally, in films involving location shoots, studio executives often require "dailies", the day's output, to be sent back via satellite in order to evaluate progress. Security is a major consideration as IP theft is rampant in the industry. The dailies might actually be sent back to the studio via satellite under protection of GeoEncryption.

Figure 9 depicts a media key distribution reference model wherein a Studio Control policy is maintained. In this model, we start with the Telecine, which produces the Digital Source Master (DSM), an uncompressed, highest resolution digital version taken from the film masters. Alternatively, this could be the output of the digital camera used in filming or the output of a digital rendering system used for CGI and animation.

Figure 9: Media Key Distribution Reference Model (Studio Control Version)



The postproduction house color corrects, edits, assembles and converts the Digital Source Master into multiple versions, possibly for presentation and exhibition on a variety of media (e.g. Theatre, DVD, Cable TV). For digital cinema distribution, the postproduction facility uses the DSM to create a Digital Cinema Distribution Master (DCDM) with appropriate resolution, color space, audio format, subtitles, captions and metadata. Each essence component (e.g., image, audio, subtitle) will be a separate data file and is known as a DCDMce.

The component DCDMce files are then optionally compressed and encrypted and then put into a standardized package or payload referred to as the Digital Cinema Package (DCP). The DCP is then optionally encrypted again for transport to the theaters. The decision to encrypt the transport stream rests with the transport/distribution provider.

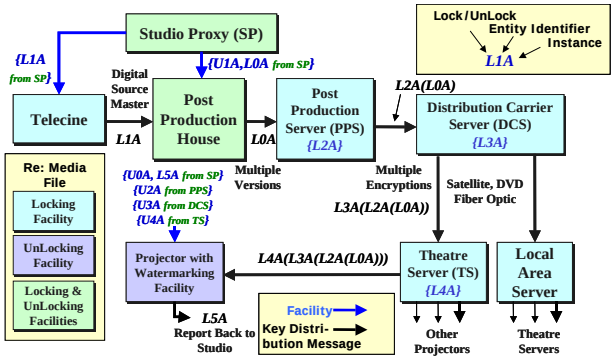
Once the DCP arrives at the theater complex, the transport stream is decrypted (if required), and the DCP is broken down into the DCDMce data files for storage on the theatre's file server. The Theatre server then provides the still encrypted media file to an authorized, tamper resistant projector, which contains sufficient buffering to source the real-time decryption and exhibition of the media file(s).

Placing four successive locks on the random key (ala. Figure 7), the studio proxy can force the key(s) to traverse the distribution carrier's server which takes off its locking layer (U4A), the Theatre server which takes off its locking layer (U3A) and finally, the projector which takes off its locking layer (U2A) and the studio's lock (U0A). Only the projector and the studio proxy can access the random key(s) needed to decrypt the media file(s). Intervening stages of distribution are critically involved in key transmittal and partial decryption, but they have no access to the plaintext media.

In examining figure 9, it is important to note the distinction between the key distribution message (black) and a locking or unlocking facility (blue). The notation accompanying the key distribution message simply indicates which locks are in effect along each path. The facilities notation indicates a node's capability with regards to locking and/or unlocking the key file as well as the source of that capability. We also note that the key distribution message can contain content in addition to a key, for example, digital signatures and certificates vouching for the source of the key.

In the studio control paradigm, the studio proxy generates all public/private key pairs and distributes appropriate portions to entities in order to provide facilities. Figure 10 depicts a variation on this scheme, the distributed control version, wherein intervening nodes apply GeoLocks rather than remove them. Under this paradigm, all of the intervening nodes must provide their corresponding unlocking facility to the projector before it can access the film.

Figure 10: Media Key Distribution Reference Model (Distributed Control Version)



Shared Access Control Using Secret Sharing

People tend to be the weakest link in security.

> On the subject of computer security: "*…the mathematics are impeccable, the computers are vincible, the networks are lousy, and the people are abysmal.*" Bruce Schneier, "Secrets & Lies, Digital Security in a Networked World

Network and computer security is rarely breeched using a brute force attack against cryptographic elements; the algorithms are simply too strong. Instead, attackers rely

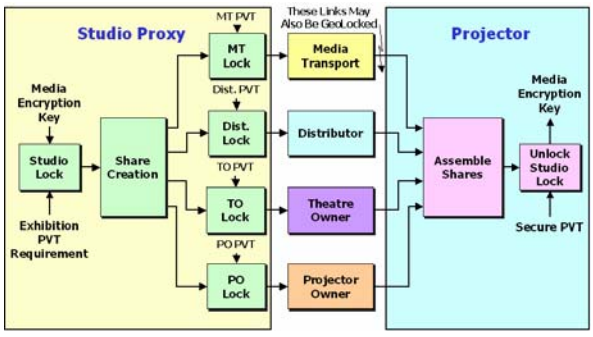
on myriad techniques that take advantage of operating systems features, attack protocols, use insider access, exploit human weaknesses, or obtain information through social engineering.

In the DoD, it has long been recognized that security is greatly enhanced by forcing distributed access control. Secure storage facilities often require two or more individuals to gain access. The simplest method is to give each individual only part of the combination lock's combination. Security is further enhanced by forcing a validation and logging procedure; for example, a call to the security guard before opening the alarmed facility to avoid an armed response.

In the civil sector, shared access control security procedures can also play a role in enforcing contract provisions. A close examination of the methods of figure 10 reveals that earlier nodes can bypass the security of the later nodes if they can gain access to the projector directly and at subsequent nodes, additional encryption is applied only to the keys and not the media file. This is typically the case for point-to-multipoint distributions where the identically encrypted media file is sent to multiple locations for reasons of cost efficiency (e.g. satellite transponder). While means have been identified for restricting access to the projector, there are more flexible alternatives.

Figure 11 depicts a mechanism for preventing bypass by incorporating a secret sharing algorithm into the key distribution process. Here, the studio proxy creates a GeoLocked key and then breaks it into shares using a secret sharing algorithm. Each share is in a sense, a part of the combination lock's combination. GeoLocked shares are then sent to the various constituents who then decode them and then forward them to the projector, possibly after performing their own GeoLocking action.

Figure 11: Distributed Access Control Using Secret Sharing



Unlike a mechanical combination lock though, there is considerable flexibility in how shares are constructed. Shares may be constructed using a "k of n" algorithm [3] where n shares are created but any set of k shares is sufficient to reconstruct the original input. Policy can be set so that no one "shareholder" can compromise the key. Similarly, policy can be set so that no one shareholder's share absence can veto the exhibition process. Alternatively, shares can be created that must be present in order for the assembly process to succeed. In effect these shares have veto powers.

Additionally, shares do not have to be created equal. As an example, one concern expressed by NATO (National Association of Theatre Owners), is the desire to avoid having so called "dark screens" in the event of a security SNAFU. Disappointing an audience is not in anyone's interest. For this reason, policy might allow the studio proxy to generate a special share, that when combined with a projector share allows the show to go on. Such a share would only be distributed on an emergency basis.

Related to this question is the issue of share validation. How does each shareholder know that they in fact have a valid share and that that share carries the stated weight in share assembly? This is important for two reasons; one is in establishing that the required shares are apriori available for the exhibition to proceed without actually assembling the shares. A second is for each shareholder to have confidence that they really have a say so regarding the exhibition in accordance with the previously agreed upon policy. Such issues can be addressed using dealer cheating detection algorithms and/or share verification [8,9].

Referring back to figures 9 & 10, we also note that the projector should report back to a security monitoring entity to allow for security violation prevention & detection. Analogous to "calling the security guard before opening the vault", this function checks to make sure the proposed share assembly is an authorized and expected event, and that it is taking place at the correct location. Enforcement may be in the form of the security monitoring entity providing its veto share only after establishing that the proposed share assembly is valid.

The projector should also maintain a security log showing all accesses to keys and subsequent exhibitions. A secure, append only security logging mechanism should be used to ensure there are no deletions in the activities log. One way to do this is to append the digital signature [10] from log entry n-1 to message n before signing it. Timestamps and locationstamps from a secure GPS can also be incorporated into the process.

Digital Watermarking

When piracy occurs, the question of WHO is obviously of extreme interest but WHEN and WHERE are also of great interest. These can help establish the WHO, and from a prosecutorial perspective, perhaps help to prove it.

GeoEncryption protects the media file from piracy at all distribution points along the path from the Studio Proxy to the Projector. Because these sites lack the keys and proper location to decrypt the media file, a pirate would be unable to acquire the plaintext. The media file is potentially vulnerable to piracy at the Projector, however, after it has been deciphered for viewing. Although the Projector can be hardened to minimize this risk, it would be desirable to have a backup mechanism in place in case such piracy occurs. Also, we need to address the problem of video cameras being used to bootleg a copy directly off of the screen. The backup mechanism could help determine the perpetrator as well as when and where the piracy took place.

Digital watermarks offer such a mechanism. In particular, the Projector could be designed to automatically watermark the media file upon decryption. The watermark could include location and time information, the projector ID, signatures, and so forth. If a pirated, watermarked media file is found, this information could provide useful evidence for establishing its source.

We also note that the same secure GPS device providing PVT values for GeoDecryption might provide signed location and time information for use in watermarking. This would ensure the integrity of the location information. In addition, the Projector might sign all of the data with its private key.

The field of digital watermarking [11] is a vast one, and beyond the scope of this paper, but a few additional comments are in order. Watermarks can be used to achieve several objectives including:

- Tamper detection
- Information hiding
- Alerting potential pirates to risk

Depending on the objective, different types of watermarking may be used. Fragile watermarks are used to detect tampering while very robust (persistent) watermarks may be used to hide information, even through several encode/decode stages, each using different standards. This is needed to ensure the bootleg copy still contains the desired information. Alerting a potential pirate to the presence of hidden watermarks may deter him, but it may also encourage him to try and sanitize his product. If the hidden information is sufficiently robust, it may survive or else, force the bootlegger to be so aggressive in his sanitization so as to render the product highly inferior.

CONCLUSIONS

Media piracy is a rapidly growing problem threatening the financial viability of the media industries. Digital distribution channels offer tremendous benefits, but with significant risks. Unless the security issues are fully addressed, the promise of digital distribution is unlikely to be fulfilled. GeoEncryption provides methods to control access to media based on location, time and velocity that builds on the foundations of more traditional cryptographic techniques. This is significant in that provides strong controls over the when and where of a media file's usage. Additionally, it discourages cloning techniques such as those that plague the DSS industry. A successful clone would operate at only one position and time frame and is therefore not particularly useful.

The specific GeoEncryption implementation discussed provides full protection against location bypass and, depending on the implementation, it also can provide strong protection against location spoofing. It also enjoys the efficiency of symmetric encryption, important in decrypting very large digital cinema files.

Adding secret sharing methods to the process further enhances security by requiring multiple entities to cooperate in order to gain access to the media file. This helps to prevent single point security failures in that it restricts each party's ability to compromise security. It also allows for very flexible security policy in terms of veto powers, share weighting, and dark screen prevention.

With a suitable method of watermarking, the GeoEncryption security framework could also support anti-piracy measures for the plaintext, even after it is properly decrypted.

Finally, we would note that GeoEncryption has applications outside of digital cinema, including military applications, virtual private networks, and infrastructure assurance [12].

ACKNOWLEDGMENTS

The authors would like to acknowledge the helpful commentary and discussions with our other GeoCodex partners: Mark Seiler, Barry Glick and Ron Karpf and the helpful inputs from Curt Behlmer of DCV.

REFERENCES

[1] FIPS 46-3
[2] FIPS 197
[3] Bruce Schneier, "Applied Cryptography, 2nd ed."
[4] Diffie & Hellman, "New Directions in Cryptography" IEEE Transactions on Information Theory, Nov 1976
[5] SEP discussions at: http://home.earthlink.net/~loganscott53/Circular_Error_Probable.htm
[6] Logan Scott, Navtech Seminars course: "GPS Interference & Jamming Issues for Civil & Military Users"
[7] Logan Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems" presented at this conference, ION-GPS-2003
[8] Chang & Chen, "Detecting Dealer Cheating in Secret Sharing Systems", 0-7695-0792-1/00 IEEE
[9] Wenbo Mao, "Necessity and Realization of Universally Verifiable Secret Sharing"
[10] see for example FIPS PUB 186-2: DIGITAL SIGNATURE STANDARD (DSS)
[11] Voyatzis & Pitas, "The Use of Watermarks in the Protection of Digital Multimedia Products" PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999
[12] Logan Scott & Dorothy Denning, "A Location Based Encryption Technique and Some of Its Applications", ION-NTM-2003